量子信息引论*

郭 光 灿

(中国科学技术大学量子通信与量子计算开放研究实验室 合肥 230026)

摘 要 文章在简述量子信息的发展背景之后,介绍了量子纠缠、量子计算、量子密码、量子因特网、量子克隆、量子对策论等方面的内容,既阐述了相关的基本概念,也论及最新的研究进展.

关键词 量子信息,量子通信,量子计算,量子对策论

INTRODUCTION TO QUANTUM INFORMATION

GUO Guang-Can

(*Laboratory of Quantum Communication and Quantum Computation, University of Science and Technology of China, Hefei* 230026, *China*)

Abstract After an introduction to the background of quantum information we review the main topics in this field, including quantum entanglement, quantum computation, quantum cryptography, quantum communication, quantum cloning and quantum game theory. We deseribe not only the relevant basic concepts, but also new developments in quantum information research.

Key words quantum information, quantum communication, quantum computation, quantum game theory

1 引言

量子信息是信息科学与量子力学相结合的新兴交叉学科,开拓了量子力学应用的新天地,为 21 世纪信息科学的发展提供了新的原理和方法.

著名物理学家费恩曼(Feynman)曾指出:量子力学的精妙之处在于引入几率幅(即量子态)的概念.事实上,量子世界的千奇百怪的特性正是起源于这个量子态.而量子理论的长期激烈争论的焦点也在于这个量子态.量子信息科学采用这个奇妙的量子态作为信息单元(称为量子比特).量子比特是两态量子系统的任意叠加态:

$$|\psi\rangle = C_0|0\rangle + C_1|1\rangle, \quad |C_0|^2 + |C_1|^2 = 1,$$

式中$|0\rangle$和$|1\rangle$为正交态,通常称为计算基态或数据态.

量子比特的物理载体是任何两态的量子系统,如光子、电子、原子、原子核、声子等等.一旦用量子态来表示信息,便实现了信息的"量子化",于是信息的过程必须遵从量子物理原理.例如信息传输是指量子态在通道中的传送,信息处理便是指对量子态实行相应的幺正变换,而信息提取则是对量子信息系统实施量子测量.

因此,量子世界的奇妙特性(如叠加性、相干性、纠缠性、不可克隆定理等)会在信息过程中发挥出重要作用,使量子信息系统的信息功能突破现有经典信息系统的极限.例如,量子计算机可攻破现有的密码体系,量子密码能提供绝对安全的保密通信系统,量子因特网可构造性能独特的新型通信网络.

国际著名的量子信息权威 Bennett 于 2000 年曾在《Nature》上发表一篇评述性文章[1],他精辟地指出,从经典信息到量子信息的推广,就象从实数到复数的推广一样.

量子信息的基体是经典信息和量子纠缠,两者具有截然不同的特性:经典信息可以克隆,但只能沿着时间箭头方向传播,而量子纠缠不可克隆,但却能把时空中的任意两点联系起来.所以,量子信息除研究诸如计算、传输等传统内容之外,还萌生出如量子对策、量子通信复杂性等新的课题.

* 国家自然科学基金(批准号:19874056)资助项目
2001 - 01 - 22 收到

2 量子纠缠

量子纠缠是存在于多子系的量子系统中的一种奇妙现象,即对一个子系统的测量结果无法独立于对其他子系统的测量参数.虽然近些年来,随着量子信息的蓬勃发展,量子纠缠逐渐成为人们的热门话题,但它并不是什么新事物."纠缠"这一名词的出现可以追溯到量子力学诞生之初.例如,在爱因斯坦等人于 1935 年提出的 EPR 佯谬[2] 中便已提出纠缠态的想法,玻尔在这个争论中也看到了,在考虑多粒子时量子理论会导致纯粹的量子效应.然而,无论是玻尔还是爱因斯坦,都没有洞悉他们所讨论的纠缠态的全部含义,在经过数十年的努力后,量子纠缠的含义才逐渐地被发掘出来[3].现在,量子纠缠态已被广泛地应用于量子信息的各个领域.

那么,什么样的量子态才算是纠缠态呢?设想有个由 A 和 B 构成的复合系统,若其量子态不能表示成为子系统态的直积则称为纠缠态,即

$$|\psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\psi\rangle_B .$$

纠缠态 $|\psi\rangle_{AB}$ 具有非局域关联特性:无论 A 与 B 在空间上分离多远,彼此都有量子关联,对 A 的测量会导致 B 的量子态的坍缩(EPR 效应).

Bell 态是两态的两粒子系统的最大纠缠态:

$$\begin{cases} |\phi^{\pm}\rangle = \dfrac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \\ |\psi^{\pm}\rangle = \dfrac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \end{cases}$$

它们构成四维空间中的正交完备基,若采用这组基对任意态 $|\psi\rangle_{AB}$ 实施正交测量,称为 Bell 基测量.每个 Bell 态携带非局域的两比特信息:

宇称比特 (parity bit):$|\phi\rangle$ 代表偶宇称,$|\psi\rangle$ 代表奇宇称;

相位比特 (phase bit):分别由 + 、 - 来表征.

仅依靠单个子系统的任意操作均无法提取这两比特信息.借助于联合操作才可能提取编制于两个量子比特关联之中的比特信息.如下面的简单量子网络可以实现 Bell 态测量(见图 1).

对单个粒子可实施如下的局域变换:

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

若对 Bell 态实施局域操作,可实现 Bell 态之间的变换:

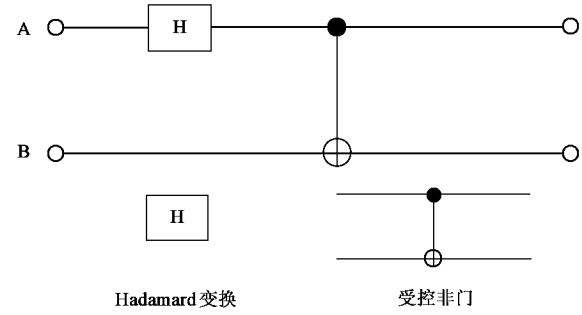

图 1 识别 Bell 态的量子网络

$$\sigma_3 : |\phi^+\rangle \leftrightarrow |\phi^-\rangle, |\psi^+\rangle \leftrightarrow |\psi^-\rangle,$$

$$\sigma_1 : |\phi^+\rangle \leftrightarrow |\psi^+\rangle, |\psi^-\rangle \leftrightarrow |\psi^-\rangle,$$

$$\sigma_2 \Leftrightarrow \sigma_1\sigma_3 : |\phi^+\rangle \rightarrow |\psi^-\rangle, |\phi^-\rangle \rightarrow |\psi^+\rangle.$$

这些局域变换无法改变每个粒子(A,B)的状态,它们均为 $\rho_A = \rho_B = I/2$.故局域操作可以编制经典比特信息于 Bell 态之中,但局域操作无法提取所编制的比特,只有联合操作才能提取信息.

两粒子纯纠缠态的纠缠度可用其子系统的 von Neumann 熵来度量,但两粒子混合态以及多粒子纠缠态的纠缠度应如何度量仍未解决,于是出现了诸如"束缚纠缠"、"可蒸馏纠缠"、"纠缠激活"等有趣的研究课题.

局域操作无法产生纠缠,纠缠态的产生需要集体操作,如相互作用和纠缠交换等.我们实验室在实验上采用参量下转换过程研制成功脉冲和连续的光子纠缠态,并演示了其双光子干涉.

3 量子计算

量子比特可以制备在两个逻辑态 0 和 1 的相干叠加态,换句话说,它可以同时存储 0 和 1.考虑一个 N 个物理比特的存储器,若它是经典存储器,则它只能存储 2^N 个可能的数据当中的任一个,若它是量子存储器,则它可以同时存储 2^N 个数据,而且随着 N 的增加,其存储数据的能力将指数上升,例如,一个 250 量子比特的存储器(由 250 个原子构成),可能存储的数据比现有已知的宇宙的全部原子数目还要多.可见量子存储器具有巨大存储数据的能力.

由于运算是对存储数据进行操作(变换),因此量子计算机对 N 个量子存储器实行一次操作可以同时对所存储的 2^N 个输入数据进行数学运算,其效果等效于经典计算机要重复实施 2^N 次操作,或者采用 2^N 个不同的处理器实行并行操作.这便是量子并

行计算能力的物理基础.因此,量子计算可有效加速经典函数的运算速度.

量子计算的实现必须解决3个关键性问题:其一是量子算法,这是有效提高运算速度的关键;其二是量子编码,它是进行可靠运算的保证;其三是量子逻辑网络,它是进行量子计算的物理器件.

3.1 量子算法

目前具有广泛影响的典型算法是Shor算法和Grover算法.

3.1.1 Shor算法[4]

Shor于1994年发现的Shor算法可以有效地用来进行大数因子分解.大数因子分解是现在广泛用于电子银行、网络等领域的公开密钥体系RSA安全性的依据.采用现有计算机对数N(二进制长度为$\log N$)做因子分解,其运算步骤(时间)随输入长度$\log N$指数增长.

Shor算法的主要思想是,首先利用数论中的一些定理,将大数因子分解转化为求一个函数周期问题,而后者可以用量子快速傅里叶变换在多项式步骤内完成.他证明了,利用量子计算机,可以在多项式步骤内进行大数因子分解.实验上,目前一个推广了的Shor算法已经在核磁共振中得到实现.

3.1.2 Grover量子搜索算法[5]

1997年,Grover发现了另一种很有用的量子算法,即所谓的量子搜寻算法.它适用于解决如下问题:从N个未分类的客体中寻找出某个特定的客体.经典算法只能是一个接一个搜寻,直到找到所要的客体为止,这种算法平均地讲要寻找$N/2$次,找到几率为1/2,而采用Grover的量子算法则只需要$\sqrt{N}$次.

例如,要从有10^6个号码的电话本中找出某个指定号码,该电话本是以姓名为顺序编排的.经典方法是一个个找,平均要找5×10^5次,才能以几率1/2找到所要的电话号码.Grover的量子算法每查询一次可以同时检查所有10^6个号码.由于10^6量子比特处于纠缠态,量子干涉的效应会使前次的结果影响到下一次的量子操作,这种干涉生成的操作运算重复1000(即$\sqrt{N}$)次后,获得正确答案的几率为1/2.但若再多重复操作几次,那么找到所需电话号码的几率接近于1.

Grover算法的用途很广,可以寻找最大值、最小值、平均值等,也可以用于下棋.最有趣的是可有效地攻击密码体系,如DES(the data encryption standard)体系,这个问题的实质是从$2^{56}=7\times10^{16}$个可能的密钥中寻找一个正确的密钥.若以每秒10^6密钥的运算速率操作,经典计算需要1000年,而采用Grover算法的量子计算机则只需小于4min的时间.目前,Grove算法已经在核磁共振和光学系统中得到实现.

3.2 量子模拟

除了进行上述快速计算外,量子计算机另一方面的重要用途是用来模拟量子系统.早在1982年,费恩曼(Feynman)就猜想,量子计算机可以用来模拟一切局域量子系统,这一猜想在1996年由Lloyd证明是正确的.Lloyd进一步指出,大约需要几百至几千个量子比特,即可精确地模拟一些具有连续变量的量子系统,例如格点规范理论和一些量子引力模拟.这些结果表明,模拟量子系统的演化,很可能成为量子计算机的一个主要用途.

一般地说,量子模拟可以按下列步骤来完成:(1)根据所研究的量子体系的哈密顿量,设计出能够实现相应的么正变换U的量子网络;(2)将N量子比特按照要求制备为特定初态$|\psi_0\rangle$;(3)操作计算机进行模拟运算,计算机的终态就是所需的量子态$U|\psi_0\rangle$.因此,一旦人们有了量子模拟计算机,就无需求解薛定谔方程或者采用蒙特卡罗方法在经典计算机上做数值运算,便可精确地研究量子体系的特性.

有许多量子体系可以用这种方法来研究,例如高温高密度等离子体;采用格点规范理论描述的体系(如量子色动力学);晶体固态模型(包括诸如Hubbard模型的固体费米系统);固体模型(包括诸如高温超导体的长程关联分子行为的量子模型),等等.在核磁共振中,量子模拟的初步实验业已展开.目前已经模拟了量子谐振子和反谐振子的动力学行为以及三体碰撞哈密顿量的演化.

3.3 量子编码

消相干(decoherence)是量子计算机实际应用的主要障碍,因为环境会不可避免地破坏量子相干性,使量子计算机演变成经典计算机.这个曾经困惑学术界的难题现在已经基本解决了,人们发现量子编码是克服消相干的主要途径.目前有三种不同原理的量子编码方案:量子纠错码[6]、量子避错码[7]、量子防错码[8].

量子避错码原理是我们在国际上率先提出的,其基本想法如下:

我们与英国学者独立发现在集体消相干过程中存在一类不会遭受环境破坏的特殊量子态,称为相干保持态.因此,可以将量子信息编制在这个态上,

达到无消相干存储的目的.后来美国学者证明[9],采用这类相干保持态也可以实现无消相干的可靠量子计算,而且实验上已证实这类量子态的无消相干特性[10](见图 2).

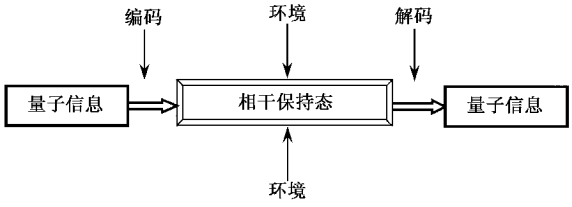

图 2　量子避错编码原理图

3.4　量子逻辑网络的物理实现

量子计算机实现的关键在于寻找适合制备量子网络的物理体系.目前在腔 QED、离子阱、核磁共振、超导系统已演示简单的量子网络,其中德、美研制成功 5 个量子比特核磁共振体系,我们已在类似体系中实现 4 个量子比特,并在探索基于光子交换的新型机制.

总之,量子计算机的实现原则上已不存在不可逾越的障碍,但技术上的实现却遇到严重的困难.如何研制多个量子比特的量子逻辑网络成为当今国际学术界关注的焦点.

4　量子密码

现代保密通信的原理图如图 3 所示.Alice 采用密钥 K(随机数)将她要发送给 Bob 的明文通过某种加密规则变换成密文,然后经由公开的经典信息通道传送给 Bob,后者采用密钥 K' 通过适当的解密规则将密文变换成为明文.这个过程如果能够有效地防止任何非法用户的窃听,那就是安全的保密通信.

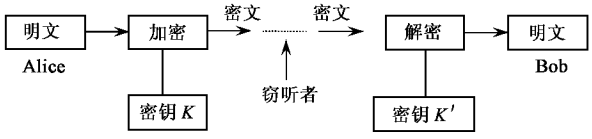

图 3　保密通信原理图

按照密钥 K 和 K' 是否相同,密钥系统可分为对称密码($K = K'$)和非对称密码($K \neq K'$).数学上证明存在有不可破译的对称密钥,即 Vernam 密码或一次性便笺式密码,它要求密钥应与明文一样长,而且仅能使用一次.这种体系需要用户双方拥有庞大的相同密码(随机数),因此密钥的传送、保管等都极不安全,不宜广泛使用.目前广泛用于网络、金融行业的是非对称密码,它是一种公开密钥,加密和解密法则、加密的密钥 K 均是公开的,只是解密的密钥 K' 不公开,只有接收者 Bob 本人知道.这种密钥的安全性基于大数因子分解这样一类不易计算的单向性函数.数学上虽没能严格证明这种密钥不可破译,但现有经典计算机几乎无法完成这种计算.

Shor 量子算法证明,采用量子计算机可以轻而易举地破译这种公开密钥体系.这就对现有保密通信提出了严峻挑战.解决这个问题的有效途径是量子密码术.量子密钥系统采用量子态作为信息载体,经由量子通道传送,在合法用户之间建立共享的密钥(经典随机数).

量子密码的安全性由量子力学原理保证.所谓绝对安全性是指窃听者智商极高,采用最高明的窃听策略,使用一切可能的先进仪器,在这些条件下,密钥仍然是安全的.窃听者的基本策略有两类:一是通过对携带着经典信息的量子态进行测量,从其测量的结果来获取所需的信息.但是量子力学的基本原理告诉我们,对量子态的测量会干扰量子态本身,因此,这种窃听方式必然会留下痕迹而被合法用户所发现.二是避开直接量子测量而采用量子复制机来复制传送信息的量子态,窃听者将原量子态传送给 Bob,而留下复制的量子态进行测量以窃取信息,这样就不会留下任何会被发现的痕迹.但是量子不可克隆定理确保窃听者不会成功,任何物理上可行的量子复制机都不可能克隆出与输入量子态完全一样的量子态来.因此,量子密码术原则上可以提供不可破译、不可窃听的保密通信体系.

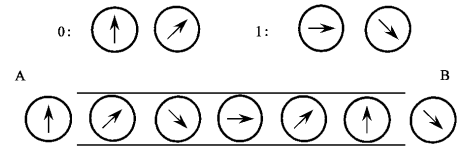

图 4　基于信源编码的 BB84 方案量子编码原理图

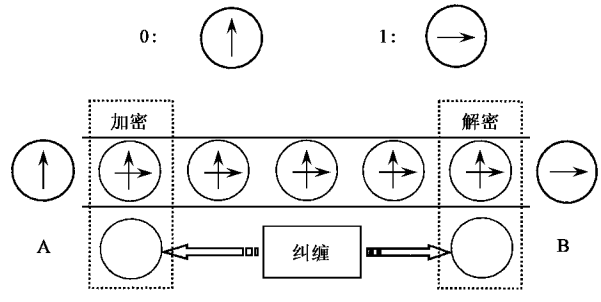

图 5　基于信道编码的量子密码原理图

现在所有的量子密码方案都是基于信源编码，即将经典随机数用非正交态来编制，基于信源编码的 BB84 方案量子编码原理见图 4. 我们提出完全新型的量子密码原理，即所谓‘信道编码”，它将两个正交态（经典信息）经由处在量子纠缠态的加密和解密器来传送密钥，这两个态在信道中以完全相同的混合态传送，窃听者无法从中获取任何信息，其安全性基于量子纠缠，进而可推广到量子信息的保密传送（见图 5）.

5 量子因特网

5.1 量子因特网

量子因特网开辟新型通信系统，可实现网络中量子信息的保密发送，多方分布计算，也可以降低通信复杂度.

量子因特网的主要部分是量子存储器（用于存储和处理信息）和量子通道（用于传输信息）（见图 6）. 例如，采用高 Q 腔中的原子作为存储器，采用光纤作为通道.

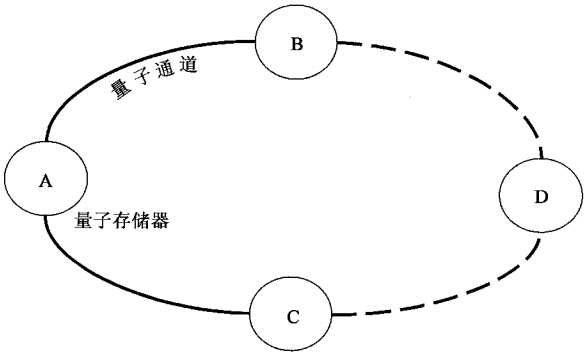

图 6 量子因特网示意图

目前学术界正致力于相关单元技术的研究，如量子隐形传态、量子密集编码、纠缠纯化等，有许多关键性课题有待解决. 例如，作为量子存储器的光腔 – 原子系统，为克服腔损耗的影响，在技术上需要在极低温下运行，且腔的 Q 值要很高，这在实验上很难实现. 最近我们提出一种易于在实验上实现的量子信息处理器，可以有效地克服光腔消相干的影响[11]. 有趣的是，在我们的文章发表两个月之后，巴黎高等师范学校的著名学者 Haroche 在实验上初步验证了我们的理论模型.

5.2 量子隐形传态

借助于 EPR 粒子对的量子通道和经典通信，可以将某个粒子的未知量子态（即量子信息）传送到远处，使另一个粒子处于这个未知量子态上，而无需传送原始粒子本身[12]. 奥地利因斯布鲁克小组首先在实验上演示光子偏振态的隐形传送[13]，美国学者在实验上演示了相干态的隐形传送. 图 7 为量子隐形传态原理图.

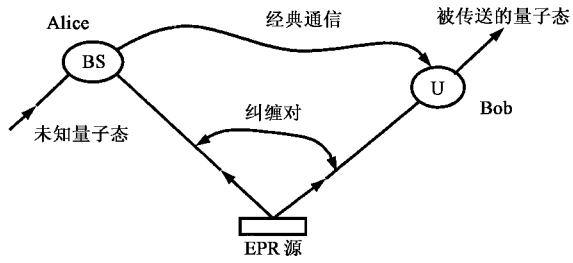

图 7 量子隐形传态原理图

5.3 通信复杂度

所谓通信复杂度是指完成某种分布计算的任务所需要的通信次数. 业已证明，采用最大纠缠的量子通道，可以有效地减低通信复杂度. 我们研究了非最大纠缠通道的通信复杂度，并用实验成功地进行了验证. 图 8 是两体计算布林函数在传送两个比特信息之后成功概率随纠缠度的变化曲线.

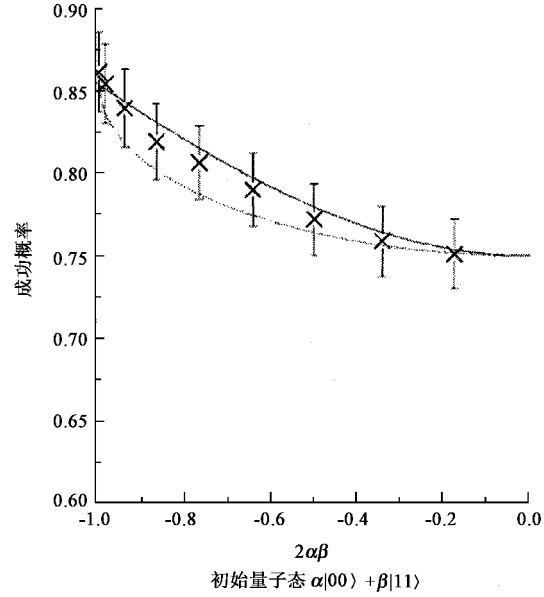

图 8 通信复杂度的实验曲线

6 量子克隆

6.1 量子不可克隆定理

1982 年，Wootters 和 Zurek 在《Nature》杂志上发表的一篇短文中提出这样一个问题[14]：是否存在一种物理过程，实现对一个未知量子态的精确复制，使

得每个复制态与初始量子态完全相同？该文证明，量子力学的线性特性禁止这样的复制，这就是量子不可克隆定理的最初表述.量子不可克隆定理的证明很简单.以两态量子系统为例，其基矢选为$|0\rangle$和$|1\rangle$，设$|s\rangle$代表此二维空间任意量子态，量子克隆过程可以表示为

$$|s\rangle|Q\rangle_x \rightarrow |s\rangle|s\rangle|\widetilde{Q}_s\rangle_x,$$

式中右端$|s\rangle|s\rangle$表示初始模和复制均处于$|s\rangle$态，$|Q\rangle_x$和$|\widetilde{Q}_s\rangle_x$分别为装置在复制前后的量子态，复制后装置的量子态$|\widetilde{Q}_s\rangle_x$可能依赖于输入态$|s\rangle$.假如存在上式的变换，那么对基矢$|0\rangle$和$|1\rangle$应该分别有

$$|0\rangle|Q\rangle_x \rightarrow |0\rangle|0\rangle|\widetilde{Q}_0\rangle_x,$$
$$|1\rangle|Q\rangle_x \rightarrow |1\rangle|1\rangle|\widetilde{Q}_1\rangle_x.$$

现假定$|s\rangle$是一个任意的叠加态，即

$$|s\rangle = \alpha|0\rangle + \beta|1\rangle, |\alpha|^2 + |\beta|^2 = 1,$$

由量子操作的线性特征，不难得到在操作后$|s\rangle$将演变为$|s\rangle|Q\rangle_x = (\alpha|0\rangle + \beta|0\rangle)|Q\rangle_x \rightarrow \alpha|0\rangle|0\rangle|\widetilde{Q}_0\rangle_x + \beta|1\rangle|1\rangle\widetilde{Q}_1\rangle_x$，如果复制机的态$|Q_0\rangle_x$与$|\widetilde{Q}_1\rangle_x$不恒等，那么上式给出的初始模和复制模均处于$|0\rangle$与$|1\rangle$的混合态；如果态$|Q_0\rangle_x$与$|\widetilde{Q}_1\rangle_x$恒等，则初始模和复制模将处于纠缠态$\alpha|0\rangle|0\rangle + \beta|1\rangle1\rangle$.无论哪种情况，初始模和复制模都不可能处于直积态$|s\rangle|s\rangle$.因此，如果一个量子复制机能精确复制态$|0\rangle$和$|1\rangle$，则它不可能复制两态的叠加态$|s\rangle$，此即量子不可克隆定理的内容.

量子态不可克隆是量子力学的固有特性，它设置了一个不可逾越的界限.量子不可克隆定理是量子信息科学的重要理论基础之一.量子信息是以量子态为信息载体(信息单元).量子态不可精确复制是量子密码术的重要前提，它确保了量子密码的安全性，使得窃听者不可能采取克隆技术来获得合法用户的信息.鉴于这个定理的重要性，近年来人们对它作了进一步的研究，揭示出更丰富的物理内涵.

量子不可克隆定理断言，非正交态不可以克隆，但它并没有排除非精确克隆即复制量子态的可能性.目前主要有两种克隆机：普适量子克隆机和概率量子克隆机.

6.2 普适量子克隆机[15]

文献中常用的是态的保真度，设输入态为$|\psi_0\rangle$，输出态为ρ，则保真度F定义为

$$F = \langle\psi_0|\rho|\psi_0\rangle.$$

普适量子克隆机(Buzek – Hillery 克隆机)对于任意的量子态都适用.其性能与输入态无关，且两个输出态完全相同，但不等于输入态，这表明输入态在复制过程中不可避免地遭到破坏.选择一组最佳参数可使得这种破坏降到最小程度，业已证明，输入、输出态之间的保真度最高可以达到5/6.我们采用了光学方法在实验上验证了量子普适克隆原理，实验结果与理论预言一致.普适量子克隆原理如图9所示.

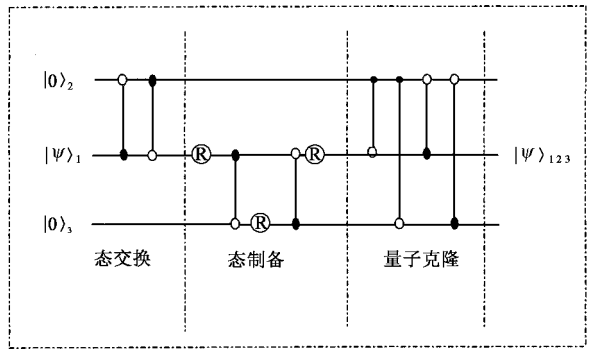

图9 普适量子克隆的原理图

6.3 概率量子克隆机[16]

概率量子克隆机原理如图10所示.概率量子克隆机适用于线性无关的态集.它把幺正演化和测量过程相结合，以确定的大于零的概率产生输出，而且输出态一定是输入态的精确复制态.为构造概率量子克隆机，测量和合适的幺正演化都是不可缺的.如果只有幺正演化，显然非正交态不可以精确克隆；另一方面，如果只有测量，当输入态为非正交态时，机器不可能对其中任意一个输入态都以大于零的概率产生输出，且输出态还是输入态的精确复制态.因此构造概率量子克隆机的关键是要设计出合适的幺正演化并要联系测量过程.概率克隆机成功产生输出的概率，定义为克隆效率，它决定了该机器的性能.显然，对于确定的输入态集合，我们希望设计一种机

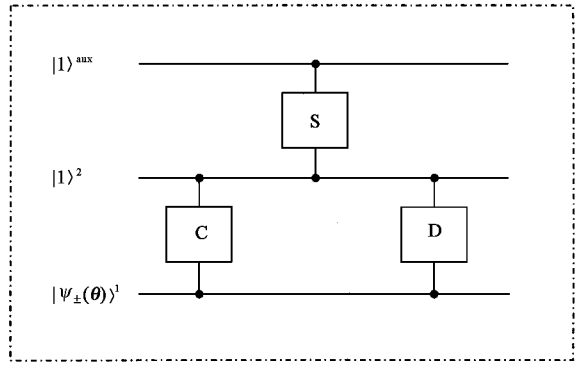

图10 概率量子克隆机原理图

器，使得它具有最大效率，且该效率不依赖于具体的输入态，此时，该机器称为最佳概率量子克隆机．概率量子克隆机保真度和克隆效率随态角的变化分别见图 11、图 12．

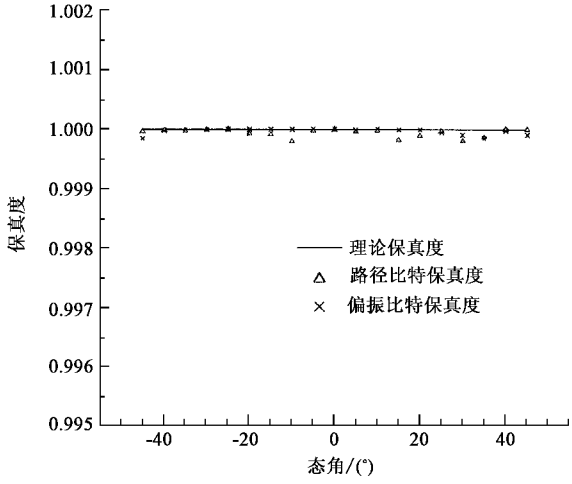

图 11　概率量子克隆机保真度随态角变化实验数据图

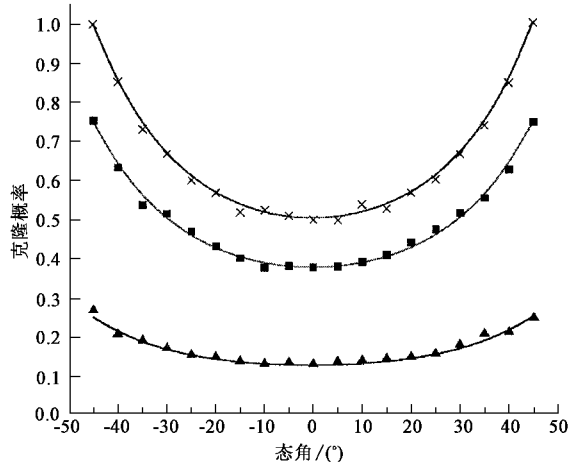

图 12　概率量子克隆机克隆效率随态角变化实验数据图
（概率克隆机的不同性能，最上面曲线对应于段－郭界限）

业已证明，如果输入态属于集合 $\{|\psi_0\rangle, |\psi_1\rangle\}$，则概率量子克隆机的最高效率为

$$\eta_{\max} = \frac{1}{1 + |\langle\psi_0|\psi_1\rangle|}.$$

显然只有对于正交输入态，该效率才能达到 1，这一点保证了基于传送两个非正交态的量子密钥体系的安全性．

7　量子对策论

量子力学应用于对策论的研究可以拓展许多有趣而新颖的课题．例如在博弈游戏中，诚实的 Alice 以等几率地朝上或朝下掷硬币于盒子中，而 Bob 猜中或猜错的几率也相同．但在经典情况下，Bob 不易检验 Alice 是否诚实．量子博弈利用量子叠加性则可以做到公正的对抗．在 PQ 翻硬币、“囚徒怪圈”等传统对策论课题中，应用量子理论可以给出十分新鲜的结果．我们采用光子网络在实验上成功演示了量子博弈机．

7.1　量子博弈

赌博中有这样一个常见的游戏：Alice 随机地往两个盒子中的一个放一个硬币（放进两个盒子的几率相等）．Bob 选中一个盒子，当 Bob 打开这个盒子，如果有硬币，Bob 赢（简单起见，假设赢一个硬币），否则 Bob 输一个硬币．但是在经典情况下，Bob 不易检验 Alice 是否按几率 $\frac{1}{2}:\frac{1}{2}$ 往盒子里放硬币，尤其在对弈次数较少的时候．但是这一游戏量子化后可以做到这一点．

量子化后的这一游戏框架如下：Alice 有两个盒子 A 和 B 用来放一个粒子．粒子在 A 盒子或 B 盒子的状态用 $|a\rangle$ 及 $|b\rangle$ 来表示．Alice 把粒子制备到某个态上，然后将盒子 B 发送给 Bob．

在下列两种情况下 Bob 赢：

（1）如果他发现粒子在 B 盒子里，Alice 检查确信粒子不在 A 盒子里，付给 Bob 一个硬币．

（2）Bob 要求 Alice 把 A 盒子发送过来，若检验到 Alice 最初制备的不是态：$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$，那么 Alice 就要付给 Bob 以 R（R 为两人事先约定的数值）个硬币．在其他情况下，Alice 赢，Bob 付给 Alice 一个硬币．

Alice 的策略就是将粒子制备到 $|\psi_0\rangle$ 态上，即粒子处在盒子 A，B 的均等叠加态上，测量后在两个盒子发现粒子的几率相等，Alice 就可以确保其收益期望值不低于 0．当然也可以将粒子制备在偏离 $|\psi_0\rangle$ 的态：$|\psi_1\rangle = \alpha|a| + \beta|b\rangle$ 上，这样就有可能被 Bob 发现，从而受罚损失 R 个硬币．

Bob 的策略是收到 B 盒子后并不立即测量粒子是否在 B 盒子里，而是先做一个变换：

$$|b\rangle = \sqrt{1-\eta}\,|b\rangle + \sqrt{\eta}\,|b'\rangle,$$

式中 $|b\rangle$ 和 $|b'\rangle$ 正交，这就好像在 B 盒子的态不破坏的情况下把粒子分成两部分，在这里分裂参数 h 依赖于惩罚参数 R．在完成态分裂操作后，Bob 做态 $|b\rangle$ 的投影测量，即查看盒子 B 里有没有 Alice 放置

的粒子.如果 Bob 发现了粒子,Bob 便赢了这一局.否则,Bob 向 Alice 索要 A 盒子用来检验:他可以用 A 盒子和留下来的$|b'\rangle$来做联合测量,即看一下粒子是否处在态$|a\rangle+\sqrt{\eta}|b'\rangle$(忽略归一化因子)上,就可以以一定的概率判断出 Alice 是否作弊.

这一量子化结果在实验上如果用一般的粒子(如原子及离子)来实现是比较困难的.我们课题组发现,如果利用光子,在现有技术下完全能够实现.我们的实验方案是利用光子经过分束器的路径来代表 A,B 两个盒子,利用光子的偏振来区别态$|b\rangle$和态$|b'\rangle$(见图 13).

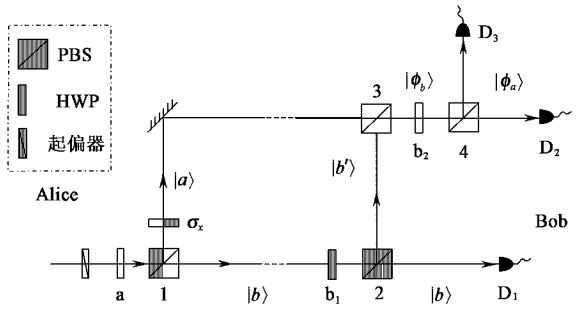

图 13 量子博弈实验原理图

7.2 量子比特承诺

在彼此极不信任且也不相信第三者的情况下,双方又要进行有效合作,"比特承诺"便成为关键性课题.Alice 向 Bob 承诺一个比特(0 或 1),并答应不会改变这个承诺,于是给 Bob 某种证据,但 Bob 不可能从这个证据中获取该承诺,只有在 Alice 帮助下 Bob 才能做到.经典比特承诺是不安全的,任何一方都可能欺骗对方而不被发现.研究量子密码术的学者们于是提出"量子比特承诺"方案,期望解决其安全性问题.但几年之后,人们证明了此方案并不安全,于是是否存在绝对安全的量子比特承诺策略便成为国际学术界感兴趣的热点.我们最近提出一种新的策略,并论证它是安全的.当然是否成功,尚待学术界评头论足之后才能获最终的认可.

8 结束语

量子信息作为新兴交叉的学科而诞生,无疑是量子力学的又一个辉煌成果,反过来也丰富了量子力学的研究内容,有力地推动量子论的发展.量子信息技术可望成为 21 世纪的重要高新技术,使信息科学从经典时代跃向量子时代.

量子信息的实现已不存在不可逾越的障碍,但在技术上实现却面临着严重困难,原因是人类迄今尚未掌握制备、保持和操控宏观尺度的量子客体的有效办法,这显然是对人类智慧和能力的又一次挑战,正是这种挑战刺激着科学家巨大的研究热情.无论对于中华民族还是年青一代,量子信息的诞生无疑是显示其聪明才智的一次难得机遇.

参 考 文 献

[1] Bennett C H, DiVincenzo D P. Nature, 2000, 404: 247
[2] Einstein A, Podolsky B, Rosen N. Phys. Rev., 1935, 47: 777
[3] Milburn G J 著, 郭光灿等译. 费曼处理器. 江西教育出版社, 1999. 49—55 [Milburn G J. Guo G C *et al*. trans. The Feynman Processor: An Introductor to Quantum Computer. Jiangxi: Jiangxi Education Press, 1999. 49—55]
[4] Shor P W. In: Proceedings of the 35th Annual Syposium on the Foundation of Computer Science. Los Alamos, CA: IEEE Computer Society Press. 1994. 124—133
[5] Grover L K. Phys. Rev. Lett., 1997, 79: 325
[6] Shor P W. Phys, Rev. Lett., 1995, 52: R2493
[7] Palma *et al*. Proc. R. Soc. London A, 1996, 452: 567; Duan L M, Guo G C. Phys. Rev. Lett., 1997, 79: 1953; Phys. Rev. A, 1998, 57: 737, 2399; Phys. Rev. A, 1998, 58: 3491
[8] Vaidman L *et al*. Phys. Rev. A, 1996, 54: R1745
[9] Lidar D A, Chuang I L, Whaley K B. Phys. Rev. Lett., 1998, 81: 2459
[10] Kwait P G *et al*. Science, 2000, 290: 498
[11] Zheng S B, Guo G C. Phys. Rev. Lett., 2000, 85: 2392
[12] Bennett C H *et al*. Phys. Rev. Lett., 1992, 69: 2881
[13] Bouwmester D *et al*. Nature, 1997, 390: 575
[14] Wootters W K, Zurek W H. Nature, 1982, 299: 802
[15] Buzek V, Hillery M. Phys. Rev. A, 1996, 54: 1844
[16] Duan L-M, Guo G-C. Phys. Rev. Lett., 1998, 80: 4999; Phys. Lett. A, 1998, 243: 261